The Quantum Threat to Bitcoin: An Analysis of Convergence with Artificial Intelligence

Renã Luiz Guarda

October 15, 2025

Abstract

This article analyzes the growing threat that quantum computing—amplified by advances in artificial intelligence (AI)—poses to the security and stability of the Bitcoin network. We investigate two main attack vectors: breaking ECDSA via Shor's algorithm and accelerating proof-of-work (PoW) mining via Grover's algorithm. We provide calculations on quantum speedups, hardware requirements, and timeline estimates, concluding that proactive migration to post-quantum cryptography is necessary.

1. Introduction

Since its creation in 2009, Bitcoin's security has been grounded in cryptographic primitives considered secure against classical computation. PoW using SHA-256 and digital ownership via ECDSA form the backbone of its robustness. Quantum computing introduces a new paradigm that threatens these foundations. We outline the threat, quantify impacts, and discuss AI's catalytic role.

2. Bitcoin's Cryptographic Foundations

Bitcoin's security depends on two primary cryptographic functions:

SHA-256: A hash function used extensively in mining. Mining seeks a nonce such that the block header hashed twice with SHA-256 has a set number of leading zeros; the difficulty of finding this nonce secures the network and regulates issuance.

ECDSA (secp256k1): Produces digital signatures proving ownership without revealing private keys. Security rests on the hardness of the elliptic-curve discrete logarithm problem (ECDLP).

3. Quantum Attack Vectors

3.1. Mining Attacks via Grover's Algorithm

Bitcoin mining is a brute-force search. Grover's algorithm yields a quadratic speedup: $O(\sqrt{(N/t)})$ versus classical $O(N/t)$. Thus a quantum miner could search much faster than ASICs. With significant quantum capacity, a malicious actor could:

- Centralize mining by consistently solving blocks faster than the network.

- Execute a 51% attack, blocking confirmations and enabling double-spends.

While difficulty adjusts every 2016 blocks, a quantum miner could wreak havoc in the ~two-week gap—mining blocks in seconds and accelerating issuance, undermining scarcity.

3.2. Fund Theft via Shor's Algorithm

Shor's algorithm solves discrete logarithms in polynomial time and can break ECDSA. Attack steps:

1. Monitor for a broadcast transaction.
2. Upon broadcast, the sender's public key is revealed.
3. Run Shor to derive the private key from the public key.
4. Spend remaining funds before the original transaction confirms.

~4 million BTC (notably in legacy P2PK outputs) have exposed public keys on-chain, making them vulnerable even without new spending.

4. Quantitative Analysis and Calculations

We contextualize the threat with calculations based on research and the Q4 2025 state of Bitcoin.

Metric	Classical Analysis	Quantum Analysis	Implication
Mining Operations	O(2^256)	O(2^128)	Quadratic speedup
ECDSA Operations	O(2^128)	O((log N)^3)	Drastically reduced complexity
Time to Break ECDSA	Billions of years	Seconds–minutes	Funds at risk
BTC at Risk (Exposed Keys)	—	~4,000,000 BTC	~$240B (at $60k/BTC)

Hardware Requirements

Quantum Mining (Grover): ~3,000–4,000 logical qubits.
Breaking ECDSA (Shor): Traditional ~2,000,000 logical qubits; recent estimates ~700 logical qubits (up to ~20× reduction reported).

5. The Role of Artificial Intelligence

Algorithmic Optimization: AI can reduce resource counts for Shor/Grover.

Error Correction: AI can search for better QEC codes.

Hardware Design: AI can optimize layouts for coherence/connectivity.

Vulnerability Analysis: AI can map exposed-key addresses and attack logistics.

6. Countermeasures and the Post-Quantum Future

- Hard fork to post-quantum signatures (e.g., CRYSTALS-Dilithium or hash-based).
- Prefer address types that hide public keys until spend (e.g., native SegWit)—does not stop real-time attacks.

7. Conclusion

Quantum + AI is Bitcoin’s most significant long-term threat. Grover can destabilize mining; Shor can catastrophically break ECDSA. Given progress and newer resource estimates, the security window is narrowing. Post-quantum defenses must be prioritized.

References

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. arXiv:1710.10377.

Benkoczi, R., Gaur, D., Nagy, N., Nagy, M., & Hossain, S. (2022). Quantum Bitcoin Mining. Entropy, 24(3), 323. https://pmc.ncbi.nlm.nih.gov/articles/PMC8946996/

Deloitte. Quantum computers and the Bitcoin blockchain. Accessed Oct 15, 2025.

CoinDesk. (May 27, 2025). Quantum Computing Could Break Bitcoin-Like Encryption Far Easier Than Initially Thought, Google Researcher Says.

Appendix — Calculations: Quantum Computing and Bitcoin

1. Quantum Speedup in Mining (Grover's Algorithm)

Classical operations (example): 2^16 = 65,536
Quantum operations (Grover): √(2^16) = 256
Speedup: 256× faster

Calculation with realistic difficulty:
Classical attempts: 2^16 = 65,536
Quantum attempts: 2^8 = 256
Real speedup: ~256×

2. Impact on Bitcoin Issuance

Normal issuance:
• Blocks per day: 144
• BTC per block: 3.125
• BTC per day: 450.00
• BTC per year: 164,250.00

Scenario with quantum miner (256×):
• Time per block: 2.3 s
• Blocks/day (pre-adjust): 36,864
• BTC/day (pre-adjust): 115,200.00
Note: difficulty adjusts every 2016 blocks (~2 weeks).

3. Breaking ECDSA (Shor's Algorithm)

ECDSA key: 256 bits
Classical: ~2^128 (infeasible)
Quantum: O(n^3) = 256^3 = 16,777,216
Est. time (1M qubits at 1 GHz): ~0.02 s
BTC at risk: ~4,000,000 (~$240B at $60k/BTC)

4. Quantum Hardware Requirements

Quantum mining: ~3,372 logical qubits (illustrative arithmetic).
Breaking ECDSA: traditional ~2,000,000; new ~700 logical qubits.

5. State vs. Requirement

Largest device: ~1,000 qubits.
ETA: mining (~3,372) ~4 years; ECDSA (~700) <1 year; old est. (2M) ~22 years.

6. Risk Analysis

Success probability: short LOW; medium MODERATE; long HIGH.
Impact: ECDSA CATASTROPHIC; mining SEVERE; confidence IRREVERSIBLE.